The Journal of the Southern Association for Information Systems

Volume 5 | Issue 1 Article 1

July 2018

The Strategic Value of Participating in Information Security Research: Evidence from the Finance, Healthcare, and Insurance Industries

Alice M. Johnson
North Carolina Agricultural and Technical State University, amjohns1@ncat.edu

The Strategic Value of Participating in Information Security Research: Evidence From the Finance, Healthcare, and Insurance Industries

INTRODUCTION

The widespread use of information technology (IT) to support business processes provides unquestionable evidence of the importance of IT for many organizations. In fact, the role of technology in organizations has surpassed its traditional administrative support role to a more strategic one that actually shapes business strategies (Henderson and Venkatraman, 1999). The mere existence of organizations such as Amazon.com, Google, e-Bay, and others are glaring examples of the modern role of technology in organizations. In fact, IT has been credited with the creation of the "ubiquitous organization – one that is everywhere, all the time" (Licker, 2006, p. 3).

Although the strategic deployment of information technology has facilitated efficiency and profitability, it has also generated a more pressing need for information security. Managers have consistently identified information security as a key issue within their organizations (Deans et al., 1991; Kumar and Palvia, 2001; Luftman, 2012; Watson et al., 1997). Furthermore, the recent surge in information security breaches has exemplified the need for better such security. For example, a large retail chain paid 18.5 million dollars in a security breach settlement (Abrams, 2017). Similarly, another breach affected 56 million customer accounts and 53 million email accounts which reportedly cost the company an estimated $80 million before insurance reimbursements (Ross, 2017). Lastly, a breach at a credit reporting organization exposed consumer credit data including personal identification information (Yu and McCoy, 2017).

Organizations have responded to the need for better security by allocating more financial resources to information security and by deploying strategic initiatives such as the implementation of more intrusion-detection tools, engaging in the active monitoring and analysis of information security intelligence, and conducting vulnerability and threat assessments. An information security study reported that 23% of the informants planned to invest in artificial intelligence and machine learning to address information security issues. Lastly, organizations experienced a 24% annual increase in their information security budgets as well as an increase in strategic initiatives to improve security and reduce risks (PWC, 2016, 2017). In fact, a recent study found that participation in an information security survey occurred because respondents perceived strategic value from doing so

(Johnson and Shipps, 2013). The ability to show strategic value from participating in information security research might help solve the challenging task of obtaining key informants to engage in such research. The remainder of this section will first discuss the current status of information security strategy and then provide the motivation for the research.

Information Security Strategy

Although the number of security breaches continues to increase and information security remains a key managerial issue, there is no consistent, agreed upon definition or criterion for developing an information security strategy. Therefore, several streams of research have provided organizations with approaches for developing such strategy. One has emphasized the importance of alignment which requires that firms establish a comprehensive information security framework that is aligned with organizational and IT strategic plans (Bowen et al., 2006).
Lack of alignment between information security strategies and organizational culture can influence the success or failure of corporate governance (Knorst et al., 2011). Such strategies must be considered when establishing and applying firm policies, training, and disciplinary practices (Solms and Solms, 2004). A recent study found marginal efforts among organizations across industries to align information security strategies with business strategies (Yaokumah, 2014).

A second stream of research has focused on deterrence which suggests the use of strategies to reduce or prevent the occurrence of security breaches. Reportedly, many such breaches occur within the organization by its disgruntled employees (Standage, 2002). Procedural and technical controls have been studied as deterrents to security breaches and abuse of IT resources. However, the results have been mixed. On one hand, Straub (1990) found that the presence of security policy statements and technical controls influenced less computer abuse. Similarly, Kankanhalli et al. (2003) found that allocating more time to security awareness activities and using advanced security software were deterrents. On the other hand, Wiant (2005) found no significant relationship between the use of security policies and the number or severity of security breaches. D'Arcy et al. (2009) found that the perceived severity of sanctions for security breaches was a more effective deterrent than the actual certainty of sanctions.

A third stream of research is aimed at providing detection methods to identify and respond to security breaches or intrusions that would compromise an organization's information resources. An intrusion may be designated as an anomaly which deviates from normal usage behavior or as a misuse which is a recognized pattern of behavior (Kumar and Spafford, 1994). Two areas widely

covered in intrusion research are (1) methods for detecting the intrusion and (2) managing and responding to the intrusion. Use of audit data generated by the operating system is the conventional, more common method for detecting intrusions (Goodall et al., 2009; Mukkamala et al., 2002). This method requires human intervention to extract characteristics of malicious intent, investigate and analyze abnormal behaviors and then enter the derived results into a detection algorithm. However, studies have delineated the benefits of using artificial intelligence, which requires less human intervention, for intrusion detection (Rehman and Saba, 2014). The technology has the ability to identify the characteristics of misuse attacks as well as identify anomalies, thus recognizing unknown suspicious events with a higher degree of accuracy than conventional intrusion methods (Abu-Nimeh et al. 2007). Artificial neural networks have been widely studied and constructed to support intrusion detection (Cansian et al, 1997; Karapilafis, 2015; Mukkamala et al., 2002). Although technologies such as artificial intelligence may limit the role of human intervention, human expertise and the knowledge base required for intrusion detection analysts remain critical (Goodall et al., 2009).

A number of guidelines exist to describe best practices and methods for managing and responding to detected intrusions. The National Institute of Standards and Technology has developed a life cycle model that describes the major phases of the incident response process (Cichonski et al. 2012). Likewise, other national and international organizations have suggested activities for effective intrusion detection and management (e.g., Brewster et al., 2012; ENISA, 2010; ISACA, 2012; ISO/IEC 27001, 2013). Nevertheless, awareness and compliance to the standards and guidelines are reportedly quite small (Tsohou et al., 2010).

Motivation for the Research

Information security research generally requires the sharing and collection of sensitive data. The challenges associated with the collection of such data have been long recognized (e.g., Hosseini and Armacost 1993; Tourangeau et al., 1998). More specifically, low response rates have been frequently reported for information security research (Hagen et al., 2011; Hall et al., 2011; Mitchell et al., 1999). For example, Kotulic and Clark (2004) were unable to complete their information security study due to the low response rate. As a result, the initial research was abandoned and replaced with the topic, "why there aren't more information security research studies" (p. 597). They further concluded that organizations might not be willing to share such sensitive information even if it could result in improvements for their organization. Hence, the current research was motivated by the need for

more information security studies as well as the preliminary Johnson and Shipps (2013) finding that organizations might participate in the research if strategic value was perceived from doing so. The ability to complete more information security research might result in more solutions to minimize the occurrence of security breaches. Because Kotulic and Clark (2004) had already delineated the reasons for non-participation in information security research, that topic was not covered in the current study. The primary objective of this study was to further investigate the strategic value of participating in information security research. For purposes of this study, information security research refers to survey research.

PREVIOUS RESEARCH

Strategic Value

Research about strategic value has focused on defining the components of the construct as well as studying its predictors and outcomes. The resource-based theory suggests that an activity has strategic value when it contributes to organizational success thereby resulting in cost reductions and/or improvements in firm performance (Barney, 1991). Zhuang and Lederer (2006) employed this theory to study the effects of human, business and e-commerce technology resources on firm competitiveness. They found that e-commerce technology and business resources predicted e-commerce performance and that e-commerce performance predicted firm performance. Similarly, other studies have employed the resource-based view to determine the extent to which IT contributed to business performance. Wade and Hulland (2004) identified eight such IT resources which were grouped into three categories and further emphasized the importance of examining resource complementarity and other moderating factors when investigating the effects of IT on firm performance. Likewise, Cao, et al., (2011) proposed a contingency resource-based view and argued that IT business value depended on the interaction of a system of variables that were subjected to multiple moderators and mediators.

Another framework, Porter's (1985) value chain model has been employed to study strategic value. Although the model does not address information security specifically, it does address activities that organizations might engage in to improve operational efficiency which is associated with operational support, a variable of interest for the current research. The strategic value of operational efficiency has been recognized as an important resource for organizations (Philip 2007; Scheraga, 2004). The value chain model used two categories to describe value-added activities that organizations could engage in to achieve competitive advantage. One

was primary activities which were directly related to the production and distribution of an organization's products and services. The other was support activities such as human resource management and procurement. In contrast to primary activities, the support activities add value indirectly by supporting primary activities. Because the value chain model helps an organization to identify core activities that facilitate firm performance, it has been widely used to study supply chain optimization in a variety of organizational contexts (e.g.., Jraisat, 2016; Reddy et al., 2013). A case study found a relationship between supply chain capabilities and value chain flexibility (Soon and Udin, 2011).

A third framework, the perceived strategic value of information systems (PSVIS), was developed by Subramanian and Nosek (2001). Its three dimension were (1) operational support which measured the extent to which information systems were used to reduce costs and enhance firm efficiency, (2) managerial productivity which measured the extent to which information systems improved manager productivity by providing better access to information, and (3) strategic decision aid which addressed the use of information systems to provide support for strategic decision-making. Following Subramanian and Nosek (2001), Grandon and Pearson (2003) validated and used the PSVIS instrument as well as other IT adoption factors to study e-commerce in small and medium sized enterprises in the midwest region of the US. They found that the perceived strategic value of e-commerce was highly associated with factors that influenced e-commerce technology. Additionally, the strategic decision aid factor was more important for perceived strategic value. Following that study, they used the PSVIS instrument to determine the factors that differentiated adopters and non-adopters of e-commerce (Pearson and Grandon, 2005). The managerial aid factor which comprised the three PSVIS dimensions was identified as a factor that differentiated adopters from non-adopters. Similar to the Grandon and Pearson (2003) and Pearson and Grandon (2005) studies, Saffu et al., (2008) studied the relationship between the perceived strategic value of e-commerce and e-commerce adoption among small and medium-sized Ghanaian firms. Their research showed that operational support was the strongest predictor of the strategic value of e-commerce adoption. The PSVIS instrument has been used extensively to study e-commerce adoption (e.g., Mishra et. al., 2012; Seyal et al., 2012; Seyal and Rahim, 2010; Lim et al., 2017). However, Verma and Bhattacharyya (2017) used it to study the adoption of big data analytics and found that a major reason for non-adoption of that technology was that firms did not realize its strategic value. Table 1 provides a summary of relevant strategic value research.

Researcher(s)	Finding(s)
Ndofor and Levitas (2004)	Developed a two dimensional framework (based on firm-level uncertainty and environmental uncertainty) that examined mechanisms firms could use to successfully transfer knowledge to key stakeholder groups while simultaneously preventing such transfer to competitors.
Fink (2011)	Business and managerial capability directly affected IT-based competitive advantage (ITCA). However, technical and behavioral capabilities indirectly affected ITCA through their effects on physical and managerial capabilities.
Berghe and Guild (2008)	A firm's perception of the strategic value of new product innovation influences the probability that the firm will secure a form of exclusive license agreement.
Saffu et al. (2007)	The perceived strategic value construct resulted in four factors: strategic decision support, information management, organizational support, and decision aids.
Morin and Hovav (2012)	Knowledge management was identified as a key factor in the adoption of Enterprise Digital Rights management technology.
Bose and Oh (2004)	An analysis of case studies identified and ranked seven strategic value drivers. They were: profitability, uniqueness of innovation, reputation of research team, growth prospects, quality of management, economic factors, and risks.
Haksever et al. 2004	A comprehensive model of value creation is proposed to describe how an organization might create value for each of its stakeholder groups.
Kwun et al. 2010	Organization compatibility, entrepreneurial mindset, and industry competitiveness influenced the perceived strategic value of e-commerce in small businesses.
Subramanian and Nosek (2001)	An instrument was developed to measure the perceived strategic value of information systems. Its dimensions were operational support, managerial productivity, and strategic decision aid.
Koh et al. (2007)	The strategic value of the Internet varies across countries.

Researcher(s)	Finding(s)
McWilliams and Siegel (2010)	Resource-based theory, economic, and pricing models are used to determine the strategic value of corporate social responsibility (CSR). An approach for quantifying the strategic value of engaging in CSR is elucidated.

Table 1. Summary of Strategic Value Research

Research Participation Factors

The ability to obtain sufficient subjects to participate in studies has long been recognized as a bottleneck that impedes research. As a result, publications, including entire books, have described techniques for acquiring such participation. The publications can be grouped into two categories. One has delineated techniques that could be applied to any discipline. For example, Dillman's (1978) seminal work provided techniques to improve participation response rates for telephone and mail surveys. His instructions for a high participation rate advised researchers to include a cover letter that clearly describes the purpose of the study, explains why the individual's participation is important, and ensures anonymity. Among other tasks, an important component of Dillman's technique was a series of follow-up correspondences to non-respondents. Subsequently, that literature was updated to include other, more modern ways to administer surveys such as the Internet and interactive voice response surveys (Dillman 2007). Groves et al., (1992, 2000, 2004) have identified a number of factors, such as incentives and perceived legitimacy of the sponsor that influenced research participation.

The second category of research has focused on issues about participation for specific areas of interest. One such study has prescribed methods for obtaining participation for health surveys (Preloran, et al., 2001). A second has identified factors that influenced participation in agricultural research (Sanginga, et al., 2006). A third has identified factors that influenced participation in information security research. Kotulic and Clark (2004) identified a number of reasons that prohibited subjects from participating in information security research. In contrast, Johnson and Shipps (2013) identified factors that motivated subjects to participate in information security survey research and suggested that the factors might vary across industries. More specifically, participants in the finance, healthcare, and insurance industries had strategic reasons for participating in information security research.

AN APPLICATION OF PERCEIVED STRATEGIC VALUE OF INFORMATION SECURITY RESEARCH PARTICIPATION

A popular belief is that organizations engage in action or behavior that is thought to add value because doing so facilitates desirable outcomes. For example, perceptions of the strategic value of e-commerce has influenced the decision to adopt that technology (Amit and Zott, 2001; Grandon and Pearson, 2003; Saffu, et al., 2008). Madu (2005) showed that the strategic value of reliability and maintainability management influenced organizational competiveness and customer satisfaction. He argued that equipment must be properly maintained and reliable to support a firm's ability to rapidly respond to customer demands and thus enhance supply chain efficiency. Lastly, several studies have consistently recognized the strategic value of information systems (IS) planning (e.g., Henderson and Sifonis, 1988; Porter, 1985; Rockart, 1979). Such planning has long been linked to achieving competitive advantage (Lederer and Mendelow, 1986; Porter and Millar, 1985; Wijaya and Manongga, 2012). Thus, the premise is that organizations engage in activities that are thought to offer strategic value.

Studies have identified several factors that influenced participation in research (e.g., Dillman, 1978, 2007; Groves, et al, 1992, 2000, 2004). However, few have focused on information security research. Furthermore, after an exhaustive review of existing literature, no studies were identified that focused specifically on the *strategic* benefits of participating in general and/or information security research. Because perceived strategic value does influence organizational behavior, it is imperative that such value be identified for participating in research endeavors. Moreover, considering the challenge associated with obtaining participants specifically for information security research (Kotulic and Clark, 2004), identifying the strategic value of such participation might help to improve the response rate. Hence, greater participation might facilitate improved security.

The current study is an extension of the Johnson and Shipps (2013) study which found that executives participated in an information security survey because they believed doing so would add value to their firms by improving the organization's ability to compete, as well as providing support for existing strategies. Subramanian and Nosek's (2001) PSVIS instrument was adapted to study the following questions:

1. Does the strategic value of participating in information security research influence the decision to participate?

2. Are some value-added activities more influential than other such activities in the decision to participate in information security research?

The PSVIS instrument was employed for this research because it had exhibited good psychometric properties in previous research (e.g., Grandon and Pearson, 2003; Pearson and Grandon, 2005; Saffu et al., 2008; Subramanian and Nosek, 2001) and it was parsimonious. The research required participation from busy, managerial-level subjects. Therefore, parsimony was desired in order to limit the amount of time needed to collect the data. Figure 1 illustrates the research model.

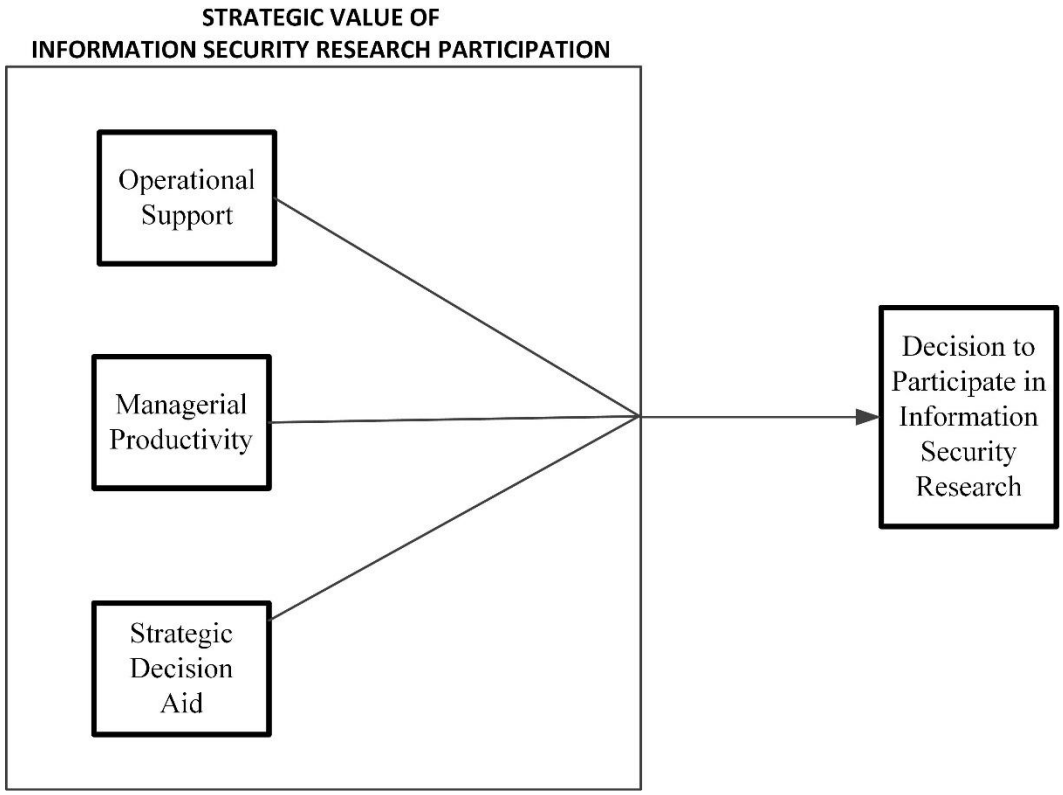

Figure 1. Research Model

METHODOLOGY

A qualitative, multiple case approach was used. This methodology was appropriate because the strategic value construct was not previously applied in this manner. Therefore, a qualitative method was appropriate to examine an area that had received limited attention in previous studies (Eisenhardt, 1989; Yin, 2016). Furthermore, this approach permitted the researcher to ask and answer "how" and "why" inquiries to delineate and clarify theory (Benbasat et al., 1987; Lee, 1989). Multiple cases were used to provide a broad, comprehensive view of the relationships under investigation.

Data Collection

Three chamber of commerce membership lists, as well as a list of US firms in the finance, healthcare, and insurance industries were used to identify potential participants. These industries were selected because prior research had suggested that individuals in those industries would be more likely to garner strategic reasons for participating than those in other industries (Johnson and Shipps, 2013). An email was sent to subjects to explain the purpose of the study and to assure anonymity. Follow-up postal contacts and phone calls were also completed. Thirteen information security managers and executives agreed to participate in the study. Each were vetted to ensure they had previously participated in other information security research prior to the current study. Such vetting was necessary because the current study required that subjects answer questions about previous participation. Also, that participation would help to produce richer feedback material from the subjects (O'Sullivan, 2010). Table 2 shows the demographics for each industry.

Industry	Number of Information Security Participants	Average Number Of Employees	Average Revenue (in billions)
Finance	6	86,189	36.84
Healthcare	4	31,500	4.29
Insurance	3	24,198	27.13

Table 2. Industry Demographics

Structured interviews were used because they are the most common method use for qualitative information systems research (Myers, 2013; Orlikowski and

Baroudi, 1991) and they allow the researcher to explore and clarify sensitive issues (Nay-Brock, 1984). Eight of the interviews were conducted face-to-face. Due to scheduling conflicts and geographical limitations, three were completed on the telephone, and two were conducted via video conferencing. The average duration for the interviews was 75 minutes. Prior to data collection, the interview manuscript was reviewed by two university professors (one had published strategic management research and the other had published information security research) and two information security executives. The feedback from each review was used to revise and finalize the interview manuscript.

Each interview started by reiterating the objectives of the research, and discussing applicable definitions. Table 3 contains the definitions.

Research Term	Definition
Information Security and information security survey research	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Kissel, 2013) Information security survey research is activity that requires a response to questions about information security. This activity could be conducted in a variety of ways (e.g., face-to-face, telephone, documented questionnaire, etc.) (Dillman, 1978, 2007)
Operational Support	Supports operational efficiency through cost reduction, improved customer service, and support to overall operations (Subramanian and Nosek, 2001)
Managerial Productivity	Provides better access to information, time management, and provides a means to use generic methods and

Research Term	Definition
	models in decision making (Subramanian and Nosek, 2001)
Strategic Decision Aid	Supports strategic decisions of managers (Subramanian and Nosek, 2001)

Table 3. Interview Definitions

Subsequent to a discussion about the definitions, the author asked and discussed responses to the following questions/items:

Question 1: How frequent do you participate in research about information security?

Question 2: When is the last time you participated in information security research?

Questions 3 – 5: Let's discuss the extent to which your participation in information security research has facilitated *construct dimension* in your organization. (Note: The phrase *construct dimension* was replaced with each of the three dimensions as shown in Figure 1 for each individual question.)

a. I want you to think about your most recent decision (prior to the current one) to participation in information security research. How (if any) did you believe your decision to participate in that research would facilitate *construct dimension*?
b. Were those expectations realized?

Question 6: This is a model that was developed to describe the strategic value of participating in information security research. (Note: The model shown in Figure 1 was displayed.) How precise (if any) does this model describe your decision to participate in information security research?

Question 7: In general, are there any other strategic reasons that have influenced your decision to participate in information security research?

After initial discussion about each construct dimension question/item, the author asked the subject to elaborate and clarify their answers to confirm understanding. Items contained in each construct dimension were used to do so. Extensive notes were taken during the interview and directly after each interview, the author reviewed and refined them. Interviews were not electronically recorded

because the first two subjects expressed concern when asked permission to do so and thus the author believed that any further requests to record might alienate the subjects and potentially affect the quality of the data collected. Use of recording devices during interviews could affect the accuracy of responses (Al-Yateem, 2012; McCambridge et al., 2014). Therefore, subsequent to the first two interviews, the author did not request permission to record. However, prior to analysis, each interviewee reviewed notes of his/her interview, provided any necessary clarifications, and confirmed the accuracy of them. These final notes were then used as raw data for analysis.

Data Analysis

Methods suggested by Yin (1994, 2009, 2016) and Eisenhardt (1989) were used to guide the data analysis process. The primary method of analysis was cross-case synthesis. First, a within-case analysis was done. Two information systems professors and the author (i.e., coders) independently reviewed the final interview notes from each case. Following Eisenhardt (1989), this activity permitted each coder to become "intimately familiar with each case as a stand-alone entity," p. 540. This activity was done multiple times while each coder recorded notes to capture key themes or concepts for each case, thus allowing the unique patterns of each case to emerge. Second, each coder generalized the patterns across the cases to determine key themes. Third, the three coders met to discuss their individual results. After sharing individual coder themes and discussion, the coders achieved 100% agreement on key themes.

DISCUSSION OF FINDINGS

The subjects did not appear to be apprehensive about participating in information security research, as evidenced by their responses to Question 1 about their frequency of participation in such research. The lowest participation recorded was "about once a year," whereas the highest was "three times annually." Two participants indicated that they try to participate whenever asked because they "understand the importance of research" and that "improvements in information security cannot be realized in the absence of research about the topic." All informants had participated in information security research within the last twelve months of their interview. Furthermore, their descriptions of their previous participation confirmed that it was indeed survey research. Thus, each were vetted to participate in the current study which was restricted to information security survey research.

The information collected and analyzed largely supported the research model. However, additional variables emerged about the influence of perceived strategic value on the decision to participate in information security research. The remainder of this section will discuss findings about the research model dimensions as well as these additional variables.

When asked about the influence of the strategic value of operational support on the decision to participate in information security research, all participants immediately discussed the need to provide information security as effectively and efficiently as possible. For example, one manager stated, "Although information security is paramount to our business, our resources for providing that security is limited. I believe my involvement in these studies have helped me to identify the most cost effective way to achieve optimal security. I value the feedback that I receive from my involvement." Another manager (in the finance industry) elaborated on her ability to use the knowledge derived from participating in information security studies to maintain abreast of emerging technologies (and techniques) that her company can employ to better serve customers and provide "peace of mind" that their data and money are safe. These findings were consistent with previous studies that have highlighted the importance of operational efficiency as it relates to firm performance (e.g., Bourlakis and Bourlakis, 2006; Sugumaran and Arogyaswamy, 2003/2004). Thus, the operational support dimension was supported.

Responses to questions about the managerial productivity dimension were most often related to the value of information sharing and access to information. This was consistent with a previous study which found that organizations were developing information sharing strategies as a component of their threat intelligence programs (PWC, 2017). In fact, Presidential Decision Directive 63 was established by the US government to encourage sharing of cyber security information among organizations (McCrohan, 2003). Several managers in the current study viewed their participation as a way to gain access to valuable information that is not normally shared beyond one's own organization. One insurance manager vehemently discussed the "vail of secrecy" that is associated with the external sharing of information regarding security while another healthcare manager stated that he frequently uses his participation as a way to identify and apply "best security practices" within his organization. He said, "Very often, my participation grants me access to leading researchers, as well as industry leaders, who are willing to talk and share information. I believe I have been able to use that information to be preventive, instead of corrective, when it comes to securing my

organization's information. I'd much rather prevent a breach, instead of dealing with the aftermath of correcting one. We handle information that must be secured. Otherwise, we'd be out of business." Hence, the managerial productivity dimension was supported.

Discussion comments were surprising about the relevance of the strategic decision aid dimension as it relates to information security research participation. Managers clearly suggested that this dimension was more influential than the other two. One information security executive stated, "It's all about being the best in my industry. I participate in any activity that can contribute to that goal. I have used the results of the studies to help my company compete." Furthermore, this informant, as well as several others, suggested that the other two dimensions might be indirectly related to the decision to participate, whereas strategic decision aid was directly related to that decision. More specifically, as stated by a bank executive, "The end goal is to amass information that will enable my organization to make better strategic decisions. Most other activities support this one." These comments were consistent with the role of business intelligence for strategic decision making (Visinescy et al., 2017) and thus provided support for the strategic decision aid dimension. Interestingly, the comments also suggested that the strategic decision aid variable might mediate the relationship between other strategic value variables and the decision to participate (Baron and Kenny, 1986) and that activities that support this dimension might be more influential than other activities, thus providing an answer for research question 2.

Finally, another surprising finding was the emergence of two other variables that might perhaps help to further explain the relationship between strategic value and the decision to participate in information security research. One was the strategic necessity dimension which was articulated by multiple informants, particularly in the healthcare and insurance industries. As emphasized by informants in these industries, their organizations are heavily regulated by federal standards that define specific procedures for maintaining the privacy and security of information because their firms must adhere to the Health Insurance Portability and Accountability Act of 1996 (i.e., HIPAA), as well as other policies and guidelines. One healthcare manager emphasized, "The entire industry dictates certain expectations when it comes to information security. My organization cannot survive if we do not conform. We need to remain viable. So, I have no choice in terms of engaging in opportunities such as research to increase my knowledge about information security. Actually, it's a requirement." Undoubtedly, information security is a strategic necessity for these organizations.

The other emerging variable was information intensity. Multiple subjects within all three industries emphasized their increased reliance on digitized products. One such manager stated, "Ninety-five percent of what we sell and rely on is information that happens to be in digital format. Most of it is sensitive information that merits the highest level of security. So, I can't afford to be disinterested about information security." This comment, as well as other similar ones, suggested that information intensity, as defined in previous studies (e.g., Drucker, 1988; Glazer, 1993; Lee and Kim, 2006), might perhaps be an intervening factor in the decision to participate in information security research.

Moreover, as described by the participants in the current study, it is reasonable to expect that information intensity and strategic necessity would moderate the relationship between strategic decision aid and the decision to participate in information security research. For example, the more information intense the firm, the stronger the relationship. Likewise, the perception of information security as a strategic necessity would also influence the relationship. Thus, the two variables are moderators (Baron and Kenny, 1986).

Participants were attentive and appeared to be genuinely interested in the research topic. Each discussed some strategic value for each of the three dimensions. Therefore, there was no opportunity to discuss lack of such value.

Based on the findings from the current study, a revised model shown in Figure 2 is offered. It shows the operational support and managerial productivity dimensions of perceived strategic value as independent variables and the strategic decision aid as a mediating variable that directly influences the decision to participate in information security research. However, two other variables (strategic necessity of information security and information intensity) moderate the relationship between strategic decision aid and the decision to participate.

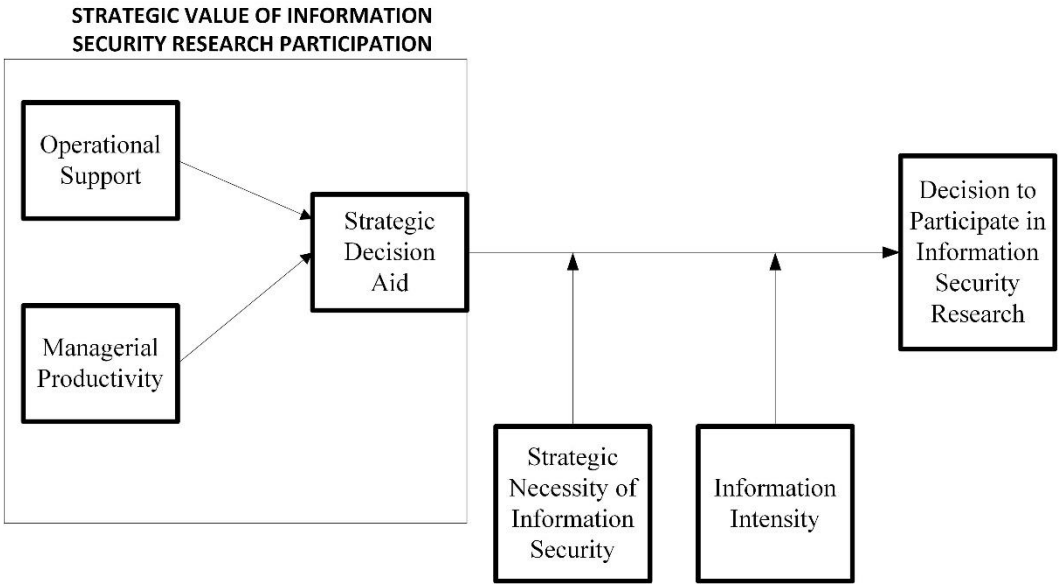

Figure 2. Revised Model of the Strategic Value of Participating In Information Security Research

RESEARCH IMPLICATIONS AND LIMITATIONS

Implications for Research and Practice

This study has several implications for research and practice. Its findings provided additional confirmation of the relationship between strategic value and the decision to participate in information security research. First, the results suggest that researchers might consider highlighting strategic, value-added benefits when soliciting for informants, particularly from the three industries included in the current study. Second, the study confirmed that the PSVIS model is appropriate for studying the decision to participate in information security research. Future researchers might build on this initial step for further theory building. For example, they could:

1. Confirm (or reject) the revised model shown in Figure 2. Also, the model could be augmented by adding a final dependent variable (e.g., organizational performance) to quantitatively assess the monetary and financial impact of participating in information security research. Doing so would help to emphasize the stakes involved in such participation.

2. Identify other "strategic value" variables, including moderating/mediating ones that might influence the decision to participate in information security research.
3. Determine if there is a relationship between perceived strategic value and the decision to participate for informants in industries other than finance, healthcare, and insurance.
4. Develop frameworks that could help researchers in their efforts to better articulate to potential informants the strategic value of participating in information security research (or perhaps research in general).

Also, the results of the current study suggested that the strategic necessity of information security and the information intensiveness of the organization might influence the decision to participate. Therefore, information security researchers might consider heavier solicitation of potential informants from information intensive industries and those industries where information security might be a strategic necessity. Doing so might perhaps result in greater participation.

Lastly, managers are more likely to engage in value-added activities. The current study might help them to more clearly understand that there is strategic value associated with participating in information security research. Because the current study employed managers who had actively participated in information security research, it emphasized *realized*, as well as perceived or intended, strategic value of participating in such research. Thus, managers who are solicited for future participation might be encouraged to think more deeply about how doing so would provide important information that could be useful for strategic decision making within their own organizations.

Limitations

This study is not without limitations. First, it must be recognized that it is an extension of a previous exploratory study that suggested that subjects in the finance, healthcare, and insurance, industries might participate in information security survey research for strategic reasons (Johnson and Shipps, 2013). Therefore, a self-selection process was employed to more precisely study the strategic benefits of such participation. Use of self-selected samples are acceptable when conducting qualitative research to discover preliminary findings that might be applied elsewhere in further research (Brinkmann et al., 2011). Other business and information systems studies have employed self-selected samples (Chan et al., 1997; Eriksson, 2014). Also, a case study methodology guided by current theory was employed to permit extensive elaboration of strategic benefits. Consequently, caution is necessary in generalizing the findings of this study to populations other

than the industries studied in this current research. Second, the sample size was small and employed a single framework (i.e., (PSVIS). Other researchers might replicate the study with a larger sample size from multiple industries and with other frameworks that delineate strategic value because doing so might disclose a more diverse outlook among the respondents.

CONCLUSION

Considering the widespread use of information technology combined with the escalating number of security breaches, information security is undoubtedly a paramount concern for practitioners, researchers, and the end consumer. Nevertheless, the ability to obtain a sufficient number of subjects for information security studies is challenging. The current study implied that potential informants might be more willing to participate if they understood the strategic value of doing so. Relationships among strategic value dimensions and the decision to participate in information security research were examined.

Potential informants beliefs about the strategic value of participating in information security research, particularly the extent to which their involvement would support strategic decision making, plays a role in the decision to participate. Therefore, researchers must do a better job articulating that value, and practitioners must also help to identify the value for their organizations.

REFERENCES

Abrams, R. (2017) Target to Pay $18.5 Million to 47 States in Security Breach Settlement, retrieved May 23, 2017 from https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html?_r=0.

Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S. (2007) A Comparison of A.I. Techniques for Phishing Detection. In: *eCrime '07: Proceedings of the Anti-Phishing Working Groups 2nd annual eCrime Researchers Summit*, ACM, New York, USA, pp 60–69.

Al-Yateem, N (2012) The Effect of Interview Recording on Quality of Data Obtained: A Methodological Reflection, *Nurse Researcher*, 19, 4, 31-35.

Amit, R. and Zott, C. (2001) Value Creation in E-business, *Strategic Management Journal*, 22, 493-520.

Barney, J. (1991) Firm Resources and Sustained Competitive Advantage, *Journal of Management*, 17, 1, 99-120.

Baron, R. M., and Kenny, D. A., (1986) The Moderator-Mediator Variable distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations, *Journal of Personality and Social Psychology*, 51, 6, 1173-1182.

Benbasat, I., Goldstein, D. K., and Mead, M. (1987) The Case Research Strategy in Studies of Information Systems, *MIS Quarterly***,** 11, 3, 369-386.

Berghe, L, and Guild, P. (2008) The Strategic Value of New University Technology and Its Impact on Exclusivity of Licensing Transactions: An Empirical Study, *Journal of Technology Transfer*, 33, 91-103.

Bose, S., and Oh, K. B. (2004) Measuring Strategic Value Drivers for Managing Intellectual Capital, *The Learning Organization*, 11, 4/5, 347-356.

Bourlakis, M., Bourlakis, C. (2006) Integrating Logistics and Information Technology Strategies for Competitive Advantage, *Journal of Enterprise Information Management*, 19, 4, 389-402.

Bowen, P., Hash, J., and Wilson, M. (2006) National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers, retrieved January 15, 2018 from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf.

Brewster, E., Griffiths, R., Lawes, A., and Sansbury, J., (2012), IT Service Management: A Guide for ITIL Foundation Exam Candidates, 2nd edition, BCS - The Chartered Institute for IT.

Brinkmann, J., Sims, R. R., and Nelson, L. J. (2011) Business Ethics Across the Curriculum? *Journal of Business Ethics Education*, 8, 83-104.

Cao, G., Wiengarten, F. and Humphreys, P. (2011) Towards a Contingency Resource-based View of IT Business Value, *Systemic Practice and Action Research*, 24, 1, 85-106.

Cansian, A.M., Moreira, E., Carvalho, A., and Bonifacio, J.M. (1997) Network Intrusion Detection Using Neural Networks, In: *International Conference on Computational Intelligence and Multimedia Applications*, 276–80.

Chan, Y. E, Huff, S. L., Barclay, D. W., and Copeland, D. G. (1997) Business Strategic Orientation, Information Systems Strategic Orientation, and Strategic Alignment, *Information Systems Research***,** 8, 2, 125-150.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K., (2012), NIST Special Publication 800 - 61: Computer Security Incident Handling Guide, revision 2, retrieved January 15, 2018 from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

D'Arcy, J., Hovav, A., and Galletta, D. (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, 20, 1, 79-98.

Deans, P.C., Karwan, K.R., Goslar, M.D., Ricks, D.A. and Toyne, B. (1991), Identification of Key International Information Systems Issues in US-based Multinational Corporations", *Journal of Management Information Systems*, 7, 4, 27-50.

Dillman, D. A. (2007) Mail and Internet surveys: The Tailored Design Method, 2nd edition, Wiley, New York.

-. (1978) Mail and Telephone Surveys: The Total Design Method, John Wiley and Sons, New York.

Drucker, P. F. (1988). The Coming of the New Organization. *Harvard Business Review*, 66, 1, 45–53.

Eisenhardt, K.M. (1989) Building Theories from Case Study Research, *Academy of Management Review*, 14, 4, 532-550.

ENISA (2010) European Network and Information Security Agency (ENISA), Good Practice Guide for Incident Management, European Network and Information Security Agency, Heraklion, Crete, Greece, retrieved March 23, 2018 from https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

Eriksson, N. (2014) User Categories of Mobile Travel Services, *Journal of Hospitality and Tourism Technology*, 5, 1, 17-30.

Fink, L. (2011) How Do IT Capabilities Create Strategic Value? Toward Greater Integration of Insights from Reductionistic and Holistic Approaches, *European Journal of Information Systems*, 20, 16-33.

Glazer, R. (1993) Measuring the Value of Information: The Information-Intensive Organization, *IBM Systems Journal*, 32, 1, 99-110.

Goodall, J. R., Lutters, W. G., and Komlodi, A. (2009) Developing Expertise for Network Intrusion Detection, *Information Technology & People*, 22, 2, 92-108.

Grandon, E. and Pearson, J. M. (2003) Strategic Value and Adoption of Electronic Commerce: An empirical Study of Chilean Small and Medium Businesses, *Journal of Global Information Technology Management*, 6, 3, 22-43.

Groves, R. M., Presser, S., and Dipko, S. (2004) The Role of Topic Interest in Survey Participation Decisions, *Public Opinion Quarterly*, 68, 1, 2-31.

-, Cialdini, R. B., and Couper, M. P. (1992) Understanding the Decision to Participate in a Survey, *Public Opinion Quarterly*, 56, 4, 475-495.

-, Singer, E., and Corning, A. (2000) Leverage-Saliency Theory of Survey Participation, *Public Opinion Quarterly*, 64, 299-308.

Hagen, J., Albrechtsen, E., and Johnsen, S.O. (2011) The Long-term Effects of Information Security E-learning on Organizational Learning, *Information Management & Computer Security*, 19, 3, 140-154.

Haksever, C, Chaganti, R, and Cook, R. (2004) A Model of Value Creation: Strategic View, *Journal of Business Ethics*, 49, 291-305.

Hall, J. H., Sarkani, S., and Mazzuchi, T. A. (2011) Impacts of Organizational Capabilities in Information Security, *Information Management & Computer Security*, 19, 3, 155-176.

Henderson, J. C. and Sifonis, J. G. (1988) The Value of Strategic IS planning: Understanding Consistency, Validity and IS markets, *MIS Quarterly*, 12, 2, 187-200.

-. and Venkatraman, N. (1999) Strategic Alignment: Leveraging Information Technology for Transforming Organizations, *IBM Systems Journal*, 38, 2&3, 472-484.

Hosseini, J. C., and Armacost, R. L. (1993) Gathering Sensitive Data in Organizations, *American Behavioral Scientist*, 36, 443-471.

ISACA (2012) Incident Management and Response, retrieved January 15, 2018 from http://www.isaca.org/Knowledge-Center/Research/Documents/Incident-Management-and-Response_whp_Eng_0312.pdf?regnum=419037.

ISO/IEC 27001 (2013) Information Technology - Security Techniques - Information Security Management Systems - Requirements, ISO/IEC 27001, Geneva, Switzerland, retrieved March 23, 2018 from https://www.iso.org/standard/54534.html.

Johnson, A. M. and Shipps, B. P. (2013) Acquiring Subject Participation for Information Security Survey Research: A Content and Correspondence Analysis approach, *Journal of Information Privacy & Security*, 9, 4, 3-30.

Jraisat, I. (2016) A Network Perspective and Value Added Tasks: The Case of Agri-food Value Chain, *Asia Pacific Journal of Marketing and Logistics***,** 28, 2, 350-365.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., and Wei, K. K. (2003), An Integrative Study of Information Systems Security Effectiveness, *International Journal of Information Management*, 23, 2, 139–154.

Karapilafis, G. (2015) Implementation of Artificial Intelligence in INFOSEC Tasks and Applications, *Journal of Applied Mathematics and Bioinformatics***,** 5, 3, 113-123.

Kissel, R.L. (2013) National Institute of Standards and Technology, Glossary of Key Information Security Terms, retrieved June 18, 2017 from https://www.nist.gov/publications/glossary-key-information-security-terms-1.

Knorst, A. M., Vanti, A. A., Andrade, R. A., E., and Johann, S. L, (2011) Aligning Information Security With the Image of the Organization Based on Fuzzy

Logic for the Industrial Automation Sector, *Journal of Information Systems and Technology Management*, 8, 3, 555-580.

Koh, C. E., Nam, K., Prybutok, V. R., Lee, S. (2007) A Value Chain Perspective of Internet Practices, E-readiness, and Organizational Performance, *Industrial Management & Data Systems*, 107, 4, 519-536.

Kotulic, A. G., and Clark, J. G. (2004) Why There Aren't More Information Security Research Studies, *Information & Management*, 41, 5, 597-607.

Kumar, A., Palvia, P. (2001) Key Data Management Issues in a Global Executive Information System, *Industrial Management & Data Systems***,** 3, 4, 153-164.

Kumar S., and Spafford, E. H. (1994) An Application of Pattern Matching in Intrusion Detection, Technical Report CSD-TR-94-013, Purdue University.

Kwun, O, Nickels, D, Alijani, G, and Omar, A. (2010) The Perceived Strategic Value of E-Commerce in the Face of Natural Disaster: E-Commerce Adoption by Small Businesses in Post-Katrina New Orleans, *International Journal of Entrepreneurship*, 14, 71-84.

Lederer, A. L. and Mendelow, A. L. (1986) Issues in Information Systems Planning, *Information & Management*, 10, 5, 245-254.

Lee, A. S. (1989) A Scientific Methodology for MIS Case Studies, *MIS Quarterly*, 13, 1, 33-50.

Lee, S. and Kim, S. E. (2006) A Lag Effect of IT Investment on Firm Performance, *Information Resources Management Journal*, 19, 1, 43-69.

Licker, P.S. (2006) Global Technology Management in the Age of Economies of Style, *Journal of Global Information Technology Management*, 9, 3, 1-4.

Lim, S. C., Baharudin, A. S., and Low, R. Q. (2017) Factors Influence SMEs in Malaysia to Adopt e-Commerce: Moderating Roles of Perceived Strategic Value, *Journal of Engineering and Applied Sciences*, 12, 6, 1566-1574.

Luftman, J., Zadeh, H. Derksen, B. Santana, M. Rigoni, E. H. (2012) Key Information Technology and Management Issues, *Journal of Information Technology*, 27, 3, 198-212.

Madu, C. N. (2005) Strategic value of Reliability and Maintainability Management, *International Journal of Quality & Reliability Management*, 22, 3, 317-328.

McCambridge, J., Witton, J., and Elbourne, D. R. (2014) Systematic Review of the Hawthorne Effect: New Concepts are Needed to Study Research Participation Effects, *Journal of Clinical Epidemiology*, 67, 3, 267-277.

McCrohan, K. F. (2003) Facing the Threats to Electronic Commerce, *The Journal of Business & Industrial Marketing*, 18, 2/3, 133-143.

McWilliams, A., and Siegel, D. S. (2010) Creating and Capturing Value: Strategic Corporate Social Responsibility, Resource-Based Theory, and Sustainable Competitive Advantage, *Journal of Management*, 37, 5, 1480-1495.

Mishra, B. B., Mishra, U. S., Mishra, U. S., and Mishra, P. K. (2012), Perception and Adoption of E-Commerce in Indian SMEs: A Study in the State of Orissa, *International Journal of Advanced Computer and Mathematical Sciences*, 3,2, 227-236.

Mitchell, R., C., Marcella, R., and Baxter, G. (1999) Corporate Information Security Management, *New Library World*, *100*, 1150, 213-227.

Morin, J., and Hovav, A. (2012) Strategic Value Drivers Behind Organizational Adoption of Enterprise DRM: The Korean Case, *Journal of Service Science Research*, 4, 143-168.

Mukkamala, S., Janoski, G., and Sung, A. (2002) Intrusion Detection Using Neural Networks and Support Vector Machines, *International Joint Conference on Neural Networks*.

Myers, M.D. (2013) Qualitative Research in Business & Management, 2nd ed., Sage Publications, London.

Nay-Brock, R. M. (1984) A Comparison of the Questionnaire and Interviewing Techniques in the Collection of Sociological Data, *Australian Journal of Advanced Nursing*, 2, 1, 14-23.

Ndofor, H. A., and, Levitas, E. (2004) Signaling the Strategic Value of Knowledge, *Journal of Management***,** 30, 5, 685-702.

Orlikowski, W.J. and Baroudi, J.J. (1991), Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information Systems Research*, 2, 1, 1-28.

O'Sullivan, T. (2010) More than Words? Conversation Analysis in Arts Marketing Research, *International Journal of Culture, Tourism and Hospitality Research*, 4, 1, 20-32.

Pearson, J.M. and Grandon, E.E. 2005, An Empirical Study of Factors that Influence E-commerce Adoption/Non-adoption in Small and Medium Sized Businesses, *Journal of Internet Commerce*, 4,4, 1-21.

Philip, G. (2007) IS Strategic Planning for Operational Efficiency, *Information Systems Management*, 24, 3, 247–264.

Porter, M. E. (1985) Competitive Advantage: Creating and Sustaining Superior Performance, Free Press, New York.

-. and Millar, V. E. (1985) How Information Gives You Competitive Advantage, *Harvard Business Review*, July-August, 149-160.

Preloran, M. H., Browner, C. H., and Lieber, E. (2001). Strategies for Motivating Latino Couples' Participation in Qualitative Health Research and Their Effects on Sample Construction, *American Journal of Public Health*, 91, 11, 1832-1841.

PWC (2016) The Global State of Information Security Survey 2016, retrieved December 16, 2015 from http://www.pwc.co.nz/PWC.NZ/media/pdf-documents/pwc-security/pwc-turnaround-and-transformation-in-cybersecurity-findings-from-gsiss.pdf.

- (2017) The Global State of Information Security Survey 2017, retrieved June 16, 2016 from http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf.

Reddy, M., Jigeesh, N., Kumar, P. (2013) Key Determinants of Successful Project Delivery in Pharmaceutical Outsourcing, *Journal of Operations Management*, 12, 3, 6-15.

Rehman, A., and Saba, T. (2014) Evaluation of Artificial Intelligent Techniques to Secure Information in Enterprises, *Artificial Intelligence Review*, 42, 4, 1029-1044.

Rockhart, J. F. (1979) Chief Executives Define Their Own Data Needs, *Harvard Business Review*, 57, 2, 81-93.

Ross, A. (2017) 11 Data Breaches that Stung US Consumers, retrieved June 21, 2017 from http://www.bankrate.com/finance/banking/us-data-breaches-1.aspx#ixzz4kH8Br7gm.

Saffu, K., Walker, J. H., and Hinson, R. (2007) An Empirical Study of Perceived Strategic Value and Adoption Constructs: The Ghanaian Case, *Management Decision*, 45, 7, 1083-1101.

-, -, and - (2008) Strategic Value and Electronic Commerce Adoption Among Small and Medium-sized Enterprises in a Transitional Economy, *Journal of Business & Industrial Marketing*, 23, 6, 395-404.

Sanginga, P. C., Tumwine, J., and Lilja, N. K. (2006) Patterns of Participation in Farmers' Research Groups: Lessons from the Highlands of Southwestern Uganda, *Agriculture and Human Values*, 23, 4, 501-512.

Scheraga, C.A. (2004) The Relationship Between Operational Efficiency and Customer Service: A Global Study of Thirty-Eight Large International Airlines, *Transportation Journal*, 43, 3, 48-58.

Seyal, A. H., Mohammad, H. A. Y. H., and Abd Rahman, M. N. (2012), Organizational Readiness, Entrepreneurship, External Pressures & Strategic Value Of E-commerce Adoption: Perceptions Of CEOs Of Bruneian SMEs, *International Journal of eBusiness and eGovernment Studies*, 4, 1, 1–12.

-, and Rahim, M.D. (2010) Understanding E-Commerce Adoption in Bruneian SMEs: A Replication of the Application of TAM and Perceived Strategic Value Models, *Journal of Electronic Commerce in Organizations*, 8, 4, 32-50.

Solms R, and Solms B. (2004) From Policies to Culture. *Computers and Security*, 23, 4, 275-279.

Soon, Q. H., and Udin, Z. M. (2011) Supply chain management from the perspective of value chain flexibility: an exploratory study, *Journal of Manufacturing Technology Management*, 22, 4, 506-526.

Standage, T. (2002) The Weakest Link, *Economist*, 365, 8296, 11–16.

Straub, D. W. (1990) Effective IS Security: An Empirical Study, *Information Systems Research*, 1, 3, 255–276.

Subramanian, G. H., and Nosek, J. T. (2001) An Empirical Study of the Measurement and Instrument Validation of Perceived Strategy Value of Information Systems, *Journal of Computer Information Systems*, 41, 3, 64-69.

Sugumaran, V., Arogyaswamy, B. (2003/2004) Measuring IT Performance: Contingency Variables and Value Modes, *Journal of Computer Information Systems*, 44, 2, 79-86.

Tourangeau, R., Smith, T., Couper, M., Baker, R., Bethlehem, J., Clark, C., Martin, J., Nicholls, W., and O'Reilly, J. (1998) Collecting Sensitive Information with Different Modes of Data Collection, Computer Assisted Survey Information Collection, John Wiley, New York.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., and Gritzalis, S. (2010) A Security Standards' Framework to Facilitate Best Practices' Awareness and Conformity, *Information Management & Computer Security*, 18, 5, 350-365.

Verma, S., and Bhattacharyya, S. S. (2017) Perceived Strategic Value-based Adoption of Big Data Analytics in Emerging Economy, *Journal of Enterprise Information Management*, 30, 3, 354-382.

Visinescu, L. L., Jones, M. C., and Sidorova, A. (2017) Improving Decision Quality: The Role of Business Intelligence, *Journal of Computer Information Systems*, 57, 1, 58-66.

Wade M. and Hulland J (2004) Review: The Resource-based View and Information System Research: Review, Extension, and Suggestion for Future Research. *MIS Quarterly*, 28, 1, 107–142.

Watson, R. T. Kelly, G. G., Galliers, R. D., Brancheau, J. C. (1997) Key Issues in Information Systems Management: An International Perspective, *Journal of Management Information Systems***,** 13, 4, 91-115.

Wiant, T. L. (2005) Information Security Policy's Impact on Reporting Security Incidents, *Computers & Security*, 24, 6, 448-459.

Wijaya, A. F. and Manongga, D. (2012) Information Systems Strategic Planning to Increase Competitive Advantage of Higher Education Using BE VISSTA Planning Methodology, *The International Journal of Organizational Innovation*, 5, 2, 68-82.

Yaokumah, W. (2014) Information Security Governance Implementation Sithin Ghanaian Industry Sectors An empirical Study, *Information Management & Computer Security*, 22, 3, 235-250.

Yin, R.K. (1994) Case Study Research, Sage Publications, Thousand Oaks, CA.

- (2009) Case Study Research Design and Methods, Fourth Edition, Sage Publications, Thousand Oaks, CA.

- (2016) Qualitative Research from Start to Finish, Second Edition, The Guilford Press, New York.

- and McCoy, K. (2017) Equifax data breach: Feds start investigation, *USA Today*, September 14, 2017.

Zhuang Y., and Lederer, A. L. (2006) A Resource-based View of Electronic Commerce, *Information & Management*, 43, 251-261.